

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-344925

(43)Date of publication of application : 14.12.1999

(51)Int.Cl.

G09C 1/00

H04L 9/14

H04L 9/34

(21)Application number : 10-166004

(71)Applicant : NEC CORP

(22)Date of filing : 29.05.1998

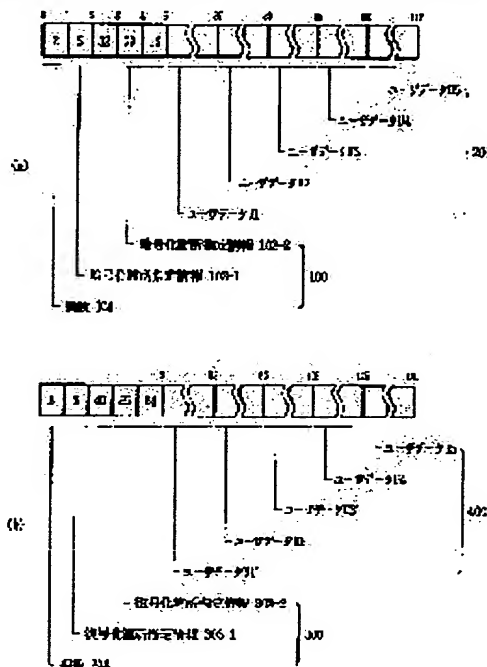
(72)Inventor : KITAMOTO YOHEI

(54) PARTIAL CIPHERING DEVICE AND RECORDING MEDIUM READABLE BY COMPUTER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a partial ciphering device capable of more finely specifying a point to be ciphered in a series of data.

SOLUTION: An information frame having a data part 200 and a ciphering control information part 100 including one or more pieces of ciphering point specification information 103-1, 103-2, in which a starting position of the data to be ciphered among a series of the data stored in the data part 200 and its length are specified and its number 104 is inputted by the partial ciphering device. And an information frame having a data part 400 in which only the data at the point specified by the ciphering control information part 100 among a series of the data is ciphered and a decoding control information part 300 in which the number of pieces of the data to be decoded, its starting position and length are specified among a series of the data stored in the data part 400 is generated and outputted.



LEGAL STATUS

[Date of request for examination] 29.05.1998

[Date of sending the examiner's decision of rejection] 13.11.2001

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-344925

(43) 公開日 平成11年(1999)12月14日

(51) Int.Cl.⁶

識別記号

F I

G 0 9 C 1/00

6 1 0

G 0 9 C 1/00

6 1 0 Z

H 0 4 L 9/14

H 0 4 L 9/00

6 4 1

9/34

6 8 1

審査請求 有 請求項の数 7 F D (全 13 頁)

(21) 出願番号 特願平10-166004

(22) 出願日 平成10年(1998) 5月29日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 北本 洋平

東京都港区芝五丁目7番1号 日本電気株式会社内

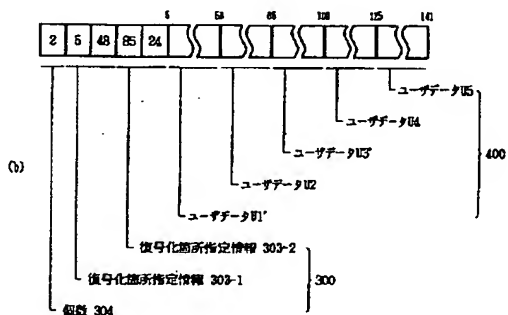
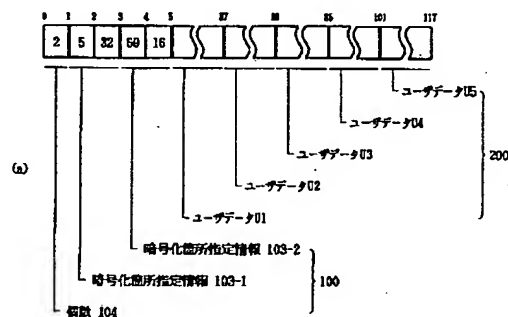
(74) 代理人 弁理士 境 廣巳

(54) 【発明の名称】 部分的暗号化装置及びコンピュータ可読記録媒体

(57) 【要約】

【課題】 一連のデータ中の暗号化したい箇所をよりきめ細かく指定することができる部分的暗号化装置を提供する。

【解決手段】 部分的暗号化装置は、データ部200 とこのデータ部200 に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した1つ以上の暗号化箇所指定情報103-1、103-2 とその個数104 とを含む暗号化制御情報部100 とを有する情報フレームを入力し、一連のデータのうち暗号化制御情報部100 で指定された箇所のデータのみを暗号化したデータ部400 と、このデータ部400 に格納された一連のデータのうち復号化対象となるデータの個数とその開始位置及び長さを指定した復号化制御情報部300 とを有する情報フレームを生成し、出力する。



【特許請求の範囲】

【請求項 1】 データ部と該データ部に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した暗号化制御情報部とを有する情報フレームを入力する入力手段と、前記一連のデータのうち前記暗号化制御情報部で指定された箇所のデータのみを暗号化したデータ部と該データ部に格納された一連のデータのうち復号化対象となるデータの開始位置及びその長さを指定した復号化制御情報部とを有する情報フレームを生成する暗号化制御手段と、前記生成された情報フレームを出力する出力手段とを備えることを特徴とする部分的暗号化装置。

【請求項 2】 前記入力手段で入力される情報フレームの暗号化制御情報部が、暗号化対象となるデータの開始位置及びその長さを指定した 1 つの暗号化箇所指定情報を含むことを特徴とする請求項 1 記載の部分的暗号化装置。

【請求項 3】 前記入力手段で入力される情報フレームの暗号化制御情報部が、暗号化対象となるデータの開始位置及びその長さを指定した 1 つ以上の暗号化箇所指定情報と該暗号化箇所指定情報の個数とを含むことを特徴とする請求項 1 記載の部分的暗号化装置。

【請求項 4】 暗号化対象となるデータを同じサイズのデータに暗号化する暗号手段を備えることを特徴とする請求項 2 または 3 記載の部分的暗号化装置。

【請求項 5】 暗号化対象となるデータをそれよりサイズの大きなデータに暗号化する暗号手段を備えることを特徴とする請求項 2 または 3 記載の部分的暗号化装置。

【請求項 6】 前記入力手段は、情報処理装置上で稼働する複数の業務プログラムのうちの任意の業務プログラムから情報フレームを入力する構成を有することを特徴とする請求項 4 または 5 記載の部分的暗号化装置。

【請求項 7】 情報処理装置を、データ部と該データ部に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した暗号化制御情報部とを有する情報フレームを入力する入力手段、前記一連のデータのうち前記暗号化制御情報部で指定された箇所のデータのみを暗号化したデータ部と該データ部に格納された一連のデータのうち復号化対象となるデータの開始位置及びその長さを指定した復号化制御情報部とを有する情報フレームを生成する暗号化制御手段、前記生成された情報フレームを出力する出力手段、として機能させるプログラムを記録したコンピュータ可読記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は暗号化装置に関し、より詳細には、一連のデータのうちの指定された箇所のみ暗号化する機能を有する部分的暗号化装置に関する。

【0002】

【従来の技術】データの暗号化は、例えば通信回線でつ

ながれた情報処理装置間でデータを送受信する場合などに機密の漏洩を防止するために実施されている。データの暗号方式には、使用する鍵の種類によって、共通鍵を使用する共通鍵方式と公開鍵を使用する公開鍵方式とに大別され、また、暗号化前後のデータサイズによって、暗号化前後で同一サイズとなる暗号方式と、暗号化によってデータサイズが拡大する暗号方式とに大別される。何れの方式でも暗号化対象となるデータ長が長くなればなるほど、暗号化処理により多くの時間がかかることにかわりはない。

【0003】そこで、同時に送信する複数のデータ間に重要度の差異がある場合、重要度の高いデータのみ暗号化し、それ以外のデータはそのまま送信することにより、暗号化処理時間を短縮することが考えられる。例えば、情報処理装置上に 2 つの業務プログラム A、B があり、業務プログラム A は図 20 (a) に示すように 1 回の送信で a 1、a 2、a 3 という 3 種類のデータを含む一連のデータを送信し、業務プログラム B は図 20

(b) に示すように 1 回の送信で b 1、b 2 という 2 種類のデータを含む一連のデータを送信し、データ a 2 とデータ b 2 とが機密情報であるとする。この場合、業務プログラム A は、データ a 1、a 2、a 3 からなる一連データを生成後、データ a 2 のみを暗号化し、得られた暗号データ a 2' と残りのデータ a 1、a 3 とで一連データを再作成して相手装置に送信する。業務プログラム B も同様に、データ b 1、b 2 からなる一連データを生成後、データ b 2 のみを暗号化し、得られた暗号データ b 2' と残りのデータ b 1 とで一連データを再作成して相手装置に送信する。こうすることにより、データ全体 (a 1 ~ a 3、b 1 ~ b 2) を暗号化するのに比べて、暗号化処理に要する時間が短縮できる。

【0004】しかしながら、以上のような部分的な暗号化処理を各業務プログラムが実施する構成では、各業務プログラムの負荷が大きくなり過ぎる。このような問題を解決するには、一連のデータのうちの指定された箇所を暗号化する機能を有する部分的暗号化装置が必要である。

【0005】このような部分的暗号化装置に応用可能な従来技術が特開平 2 - 1 8 8 7 8 2 号公報に開示されている。同公報に記載された暗号化装置は、パラメータとして、メッセージ格納域アドレス、メッセージ長、暗号処理を開始するメッセージ上の位置等を受け取って暗号化処理を実施する。暗号処理を開始するメッセージ上の位置は通常通信メッセージの開始位置が指定されており、暗号化装置は、このパラメータの指定に従い、通信ヘッダ部は暗号化せず、通信メッセージ部のみを暗号化する。

【0006】

【発明が解決しようとする課題】上述した従来の暗号化装置を応用すれば、前述した業務プログラム B の場合、

図 20 (b) に示したデータ b 1, データ b 2 からなる一連データの生成後、データ b 2 の先頭を開始位置に指定して暗号化装置に通知することにより、データ b 2 のみを暗号化した一連データを得ることができる。しかしながら、前述した業務プログラム A の場合、図 20

(a) に示したように暗号化したいデータ a 2 は中間に位置するので、データ a 2 の先頭を開始位置に指定して暗号化装置に通知すると、データ a 2 だけでなく、後続のデータ a 3 も暗号化されてしまうという問題がある。

【0007】そこで本発明の目的は、一連のデータ中の暗号化したい箇所をよりきめ細かく指定することができる部分的暗号化装置を提供することにある。

【0008】

【課題を解決するための手段】本発明の部分的暗号化装置は、データ部と該データ部に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した暗号化制御情報部とを有する情報フレームを入力する入力手段と、前記一連のデータのうち前記暗号化制御情報部で指定された箇所のデータのみを暗号化したデータ部と該データ部に格納された一連のデータのうち復号化対象となるデータの開始位置及びその長さを指定した復号化制御情報部とを有する情報フレームを生成する暗号化制御手段と、前記生成された情報フレームを出力する出力手段とを備える。

【0009】前記入力手段で入力される情報フレームの暗号化制御情報部は、暗号化対象となるデータの開始位置及びその長さを指定した 1 つの暗号化箇所指定情報を含んだ構成でも良く、暗号化対象となるデータの開始位置及びその長さを指定した 1 つ以上の暗号化箇所指定情報と該暗号化箇所指定情報の個数とを含んだ構成でも良い。また、暗号化対象となるデータを暗号化する手段は任意であり、共通鍵方式や公開鍵方式、同じサイズのデータに暗号化する暗号方式や、よりサイズの大きなデータに暗号化する暗号方式が採用できる。さらに、入力手段は、情報処理装置上で稼働する複数の業務プログラムのうちの任意の業務プログラムから情報フレームを入力することで、本発明の部分的暗号化装置が複数の業務プログラムで共通に使用できるようになっている。

【0010】

【発明の実施の形態】次に本発明の実施の形態の例について図面を参照して詳細に説明する。

【0011】図 1 は本発明を適用した情報処理装置の一例を示すブロック図である。この例の情報処理装置 1 は、通信回線 2 を介して他の情報処理装置（図示せず）と接続されており、複数の業務プログラム 3-1 ~ 3-m と、データ送受信装置 4 と、本発明にかかる部分的暗号化装置 5 および部分的復号化装置 6 とを有している。また、7 は C D - R O M, 磁気ディスク, 半導体メモリ等の機械読み取り可能な記録媒体であり、ここに記録されたプログラムは情報処理装置 1 によって読み取られ、

情報処理装置 1 の動作を制御することにより、情報処理装置 1 上に部分的暗号化装置 5 および部分的復号化装置 6 を実現する。

【0012】各々の業務プログラム 3-1 ~ 3-m は、他の情報処理装置に対して一連のデータを送信する場合、それらのデータを格納したデータ部と、このデータ部に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した暗号化制御情報部とを有する情報フレームを、送り先の情報および送り元の情報と共に部分的暗号化装置 5 に送出する。部分的暗号化装置 5 は、業務プログラム 3-1 ~ 3-m から入力した情報フレームの暗号化制御情報部を解析し、データ部中の暗号化すべき箇所のみを暗号化したデータ部と、このデータ部に格納された一連のデータのうち復号化対象となるデータの開始位置及びその長さを指定した復号化制御情報部とを有する情報フレームを生成し、送り先の情報および送り元の情報と共にデータ送受信装置 4 に送出する。データ送受信装置 4 は、入力した情報フレームに送り元の情報等を付加して、送り先の他情報処理装置に通信回線 2 を介して送信する。

【0013】他方、他の情報処理装置で同様にして作成されて通信回線 2 を介して送られてきた情報フレームをデータ送受信装置 4 が受信すると、送り先の情報および送り元の情報と共にその情報フレームが部分的復号化装置 6 に送出される。部分的復号化装置 6 は、データ送受信装置 4 から入力した情報フレームの復号化制御情報部を解析し、データ部中の復号化すべき箇所のみを復号化したデータ部と、このデータ部に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した暗号化制御情報部とを有する情報フレームを生成し、送り元の情報と共に、送り先の業務プログラム 3-1 ~ 3-m に送出する。なお、暗号化制御情報部は省略しても良い。

【0014】図 2 は部分的暗号化装置 5 の構成例を示すブロック図である。この例の部分的暗号化装置 5 は、入力手段 5 1 と、暗号化制御手段 5 2 と、暗号手段 5 3 と、出力手段 5 4 とから構成されている。入力手段 5 1 は、任意の業務プログラム 3-1 ~ 3-m から情報フレームを入力すると、それを暗号化制御手段 5 2 に渡す。暗号化制御手段 5 2 は、情報フレームの暗号化制御情報部を解析し、データ部に格納されている一連のデータのうち暗号化制御情報部で指定された箇所のデータのみを暗号手段 5 3 で暗号化し、それ以外の部分は元のままのデータとしたデータ部と、このデータ部に格納された一連のデータのうち復号化対象となるデータの開始位置及びその長さを指定した復号化制御情報部とを有する情報フレームを生成する。出力手段 5 4 は、暗号化制御手段 5 2 で生成された情報フレームを、業務プログラム 3-1 ~ 3-m から情報フレームの入力時に入力された送り先および送り元の情報を添えて、データ送受信装置 4 に

送出する。

【0015】図3は部分的復号化装置6の構成例を示すブロック図である。この例の部分的復号化装置6は、入力手段61と、復号化制御手段62と、復号手段63と、出力手段64とから構成されている。入力手段61は、データ送受信装置4から情報フレームを入力すると、それを復号化制御手段62に渡す。復号化制御手段62は、情報フレームの復号化制御情報部を解析し、データ部に格納されている一連のデータのうち復号化制御情報部で指定された箇所のデータのみを復号手段63で復号化し、それ以外の部分は元のままのデータとしたデータ部と、このデータ部に格納された一連のデータのうち暗号化対象となるデータの開始位置及びその長さを指定した暗号化制御情報部とを有する情報フレームを生成する。出力手段64は、復号化制御手段62で生成された情報フレームを、データ送受信装置4から情報フレームの入力時に入力された送り元の情報を添えて、送り先の業務プログラム3-1~3-mに送出する。

【0016】

【実施例】次に本発明の実施例について図面を参照して詳細に説明する。実施例としては、以下のものを取り上げる。

(1) 暗号化する箇所を複数指定可能な実施例

(2) 暗号化する箇所を1つのみ指定可能な実施例

また、その各々について、暗号化によりデータサイズが拡大する場合と拡大しない場合（つまり同一サイズになる場合）とについて説明する。

【0017】(1) 暗号化する箇所を複数指定可能な実施例

図4(a)は業務プログラム3-1~3-mから部分的暗号化装置5に入力される情報フレームのフォーマット例を示す図である。この例の情報フレームは、暗号化制御情報部100と、複数のユーザデータから構成されるデータ部200とから構成されている。暗号化制御情報部100は、図4(b)に示すように、データ部200に格納された一連のユーザデータのうち暗号化対象となるデータの開始位置101及びそのバイト数102を指定した1つ以上の暗号化箇所指定情報103と、この暗号化箇所指定情報103の個数104とを含む。開始位置101、バイト数102および個数104のサイズは固定長である。図4(c)に、開始位置101及びバイト数102とユーザデータとの関連、個数104と暗号化箇所指定情報103との関連を示す。開始位置101としては、例えば情報フレームの先頭の1バイト（つまり個数140の先頭バイト）目を0バイト目とした場合の、当該ユーザデータの先頭バイトまでのバイト数で表現される。なお、本実施例では、部分的復号化装置6から業務プログラム3-1~3-mに入力される情報フレームも図4(a)の形式としている。

【0018】他方、図4(d)は部分的暗号化装置5か

らデータ送受信装置4に入力される情報フレームのフォーマット例を示す図である。この例の情報フレームは、復号化制御情報部300と、複数のユーザデータから構成されるデータ部400とから構成されている。復号化制御情報部300は、図4(e)に示すように、データ部400に格納された一連のユーザデータのうち復号化対象となるデータの開始位置301及びそのバイト数302を指定した1つ以上の復号化箇所指定情報303と、この復号化箇所指定情報303の個数304とを含む。開始位置301、バイト数302および個数304のサイズは固定長である。開始位置301としては、例えば情報フレームの先頭の1バイト（つまり個数304の先頭バイト）目を0バイト目とした場合の、当該ユーザデータまでのバイト数で表現される。なお、本実施例では、データ送受信装置4から部分的復号化装置6に入力される情報フレームも図4(d)の形式としている。

【0019】(A) 暗号化によりデータサイズが拡大する場合

【0020】(ア) 暗号化

この場合の部分的暗号化装置5の処理の一例を図5のフローチャートに示す。何れかの業務プログラム3-1~3-mから図4(a)に示したような形式の情報フレームが送られると、入力手段51がそれを入力し（ステップS1）、暗号化制御手段52に伝達する。暗号化制御手段52は、情報フレームの暗号化制御情報部100を解析し（ステップS2）、解析結果を制御テーブルに設定する（ステップS3）。

【0021】例えば、図6に示すように、各々32バイト、32バイト、16バイト、16バイト、16バイトである5つのユーザデータU1、U2、U3、U4、U5を含むデータ部200と、ユーザデータU1、U3を暗号化対象として指定した2つの暗号化箇所指定情報103-1、103-2と個数「2」とを含む暗号化制御情報部100とから構成される情報フレームの場合、個数、開始位置、バイト数のサイズを例えば1バイト固定とすると、情報フレームの先頭から5~37バイト目のユーザデータU1と69~85バイト目のユーザデータU3とが暗号化対象データであり、ユーザデータU1とユーザデータU3との間のユーザデータU2、ユーザデータU3より後ろのデータ（ユーザデータU4、U5）は暗号化対象データでないので、例えば図7に示すような4つのエン트리E1、E2、E3、E4を持つ制御テーブル900を生成し、開始位置、バイト数、暗号化の有無の欄にそれぞれ図示する値を設定する。なお、この時点では、暗号化後の開始位置、暗号化後のバイト数の欄はNULLである。

【0022】次に暗号化制御手段52は、制御テーブル900の暗号化の有無の欄が「有」になっているエン트리E1、E3毎に、該当する箇所のデータをデータ部200から取り出し、暗号手段53に与えることにより暗

号化する（ステップ S 4）。

【0023】次に暗号化制御手段 5 2 は、暗号化後のデータサイズを図 7 に示すように、エントリ E 1、E 3 の暗号化後のバイト数の欄に設定し、それに基づいて暗号化後の開始位置の欄に値を設定する（ステップ S 5）。例えば、エントリ E 1 の暗号化後のバイト数は「48」に拡大したので、エントリ E 2 の暗号化後の開始位置は「53」に設定される。

【0024】次に暗号化制御手段 5 2 は、図 7 の制御テーブル 9 0 0 の暗号化の有無の欄が「有」になっているエントリ E 1、E 3 の個数「2」を個数 3 0 4、エントリ E 1 の暗号化後の開始位置「5」と暗号化後のバイト数「48」との組、エントリ E 3 の暗号化後の開始位置「85」と暗号化後のバイト数「24」との組をそれぞれ復号化箇所指定情報 3 0 3 - 1、3 0 3 - 2 とした復号化制御情報部 3 0 0 を生成する（ステップ S 6）。これにより、図 6（b）に示す復号化制御情報部 3 0 0 が生成される。

【0025】次に暗号化制御手段 5 2 は、図 7 の制御テーブル 9 0 0 のエントリ E 1 から順にエントリ E 4 ま

で、そのエントリの暗号化の有無の欄が「有」であれば暗号化後のデータを、「無」であれば、制御テーブル 9 0 0 の開始位置の欄とバイト数の欄とで特定される入力情報フレーム上の元のデータを、データ部の先頭から順に詰め込んで、データ部 4 0 0 を生成する（ステップ S 7）。これにより、図 6（b）に示すデータ部 4 0 0 が生成される。

【0026】以上のようにして復号化制御情報部 3 0 0 とデータ部 4 0 0 とから構成される情報フレームが生成されると、出力手段 5 4 が、送り先および送り元の情報

と共に情報フレームをデータ送受信装置 4 に送る（ステップ S 8）。

【0027】（イ）復号化

この場合の部分的復号化装置 6 の処理の一例を図 8 のフローチャートに示す。データ送受信装置 4 から図 4

（d）に示したような形式の情報フレームが送られると、入力手段 6 1 がそれを入力し（ステップ S 1 1）、復号化制御手段 6 2 に伝達する。復号化制御手段 6 2 は、情報フレームの復号化制御情報部 3 0 0 を解析し（ステップ S 1 2）、解析結果を制御テーブルに設定する（ステップ S 1 3）。

【0028】例えば、入力された情報フレームが図 6

（b）に示した情報フレームであった場合、情報フレームの先頭から 5 ～ 5 3 バイト目のユーザデータ U 1' と 8 5 ～ 1 0 9 バイト目のユーザデータ U 3' とが復号化対象データであり、ユーザデータ U 1' とユーザデータ U 3' との間のユーザデータ U 2、ユーザデータ U 3' より後ろのデータ（ユーザデータ U 4、U 5）は復号化対象データでないので、例えば図 9 に示すような 4 つのエントリ E 1、E 2、E 3、E 4 を持つ制御テーブル 9

0 1 を生成し、開始位置、バイト数、復号化の有無の欄にそれぞれ図示する値を設定する。なお、この時点では、復号化後の開始位置、復号化後のバイト数の欄は N U L L である。

【0029】次に復号化制御手段 6 2 は、制御テーブル 9 0 1 の復号化の有無の欄が「有」になっているエントリ E 1、E 3 毎に、該当する箇所のデータをデータ部 4 0 0 から取り出し、復号手段 6 3 に与えることにより復号化する（ステップ S 1 4）。

【0030】次に復号化制御手段 6 2 は、復号化後のデータサイズを図 9 に示すように、エントリ E 1、E 3 の復号化後のバイト数の欄に設定し、それに基づいて復号化後の開始位置の欄に値を設定する（ステップ S 1 5）。例えば、エントリ E 1 の復号化後のバイト数は「32」なので、エントリ E 2 の復号化後の開始位置は「37」に設定される。

【0031】次に復号化制御手段 6 2 は、図 9 の制御テーブル 9 0 1 の復号化の有無の欄が「有」になっているエントリ E 1、E 3 の個数「2」を個数 1 0 4、エントリ E 1 の復号化後の開始位置「5」と復号化後のバイト数「32」との組、エントリ E 3 の復号化後の開始位置「69」と復号化後のバイト数「16」との組をそれぞれ暗号化箇所指定情報 1 0 3 - 1、1 0 3 - 2 とした暗号化制御情報部 1 0 0 を生成する（ステップ S 1 6）。これにより、図 6（a）に示す暗号化制御情報部 1 0 0 が生成される。

【0032】次に復号化制御手段 6 2 は、図 9 の制御テーブル 9 0 1 のエントリ E 1 から順にエントリ E 4 ま

で、そのエントリの復号化の有無の欄が「有」であれば復号化後のデータを、「無」であれば、制御テーブル 9 0 1 の開始位置の欄とバイト数の欄とで特定される入力情報フレーム上の元のデータを、データ部の先頭から順に詰め込んで、データ部 2 0 0 を生成する（ステップ S 1 7）。これにより、図 6（a）に示すデータ部 2 0 0 が生成される。

【0033】以上のようにして暗号化制御情報部 1 0 0 とデータ部 2 0 0 とから構成される情報フレームが生成されると、出力手段 6 4 が、送り元の情報と共に送り先の業務プログラムに送る（ステップ S 1 8）。

【0034】（B）暗号化によりデータサイズが拡大しない場合

【0035】（ア）暗号化

この場合の部分的暗号化装置 5 の処理の一例を図 1 0 のフローチャートに示す。何れかの業務プログラム 3 - 1 ～ 3 - m から図 4（a）に示したような形式の情報フレームが送られると、入力手段 5 1 がそれを入力し（ステップ S 2 1）、暗号化制御手段 5 2 に伝達する。暗号化制御手段 5 2 は、情報フレームの暗号化制御情報部 1 0 0 を解析し、個数 1 0 4 を変数 M a x に、初期値 1 を変数 i に設定する（ステップ S 2 2）。例えば図 6（a）

に示した情報フレームの場合、Max は 2 に設定される。

【0036】次に暗号化制御手段 52 は、暗号化制御情報部 100 における先頭から変数 i の値番目の暗号化箇所指定情報が示す箇所のデータを、データ部 200 から取り出し（ステップ S23）、暗号手段 53 に与えることにより暗号化する（ステップ S24）。そして、生成された暗号データで、データ部 200 の元の箇所を上書きする（ステップ S25）。

【0037】これで、1 つの暗号化対象データについての処理を終えたことになり、変数 i を +1 し（ステップ S26）、Max 以下ならばステップ S23 に戻って上述した処理を繰り返す。変数 i が Max より大きければ、全ての暗号化対象データの処理を終えたので、データ部が上書きされた情報フレームを、出力手段 54 により、送り先および送り元の情報と共にデータ送受信装置 4 に送出する（S28）。

【0038】このように暗号化によってデータサイズが拡大せず同一サイズとなる場合、入力された情報フレームの暗号化制御情報部 100 の内容は実質的に変更されず、そのまま復号化制御情報部 300 となる。

【0039】(イ) 復号化

この場合の部分的復号化装置 6 の処理の一例を図 11 のフローチャートに示す。データ送受信装置 4 から図 4 (d) に示したような形式の情報フレームが送られると、入力手段 61 がそれを入力し（ステップ S31）、復号化制御手段 62 に伝達する。復号化制御手段 62 は、情報フレームの復号化制御情報部 300 を解析し、個数 304 を変数 Max に、初期値 1 を変数 i に設定する（ステップ S32）。例えば図 6 (b) に示した情報

フレームの場合、Max は 2 に設定される。

【0040】次に復号化制御手段 62 は、復号化制御情報部 300 における先頭から変数 i の値番目の復号化箇所指定情報が示す箇所のデータを、データ部 400 から取り出し（ステップ S33）、復号手段 63 に与えることにより復号化する（ステップ S34）。そして、生成された復号データで、データ部 400 の元の箇所を上書きする（ステップ S35）。

【0041】これで、1 つの復号化対象データについての処理を終えたことになり、変数 i を +1 し（ステップ S36）、Max 以下ならばステップ S33 に戻って上述した処理を繰り返す。変数 i が Max より大きければ、全ての復号化対象データの処理を終えたので、データ部が上書きされた情報フレームを、出力手段 64 により、送り元の情報と共に送り先の業務プログラムに送出する（S38）。

【0042】このように復号化によってデータが拡大せず同一サイズとなる場合、入力された情報フレームの復号化制御情報部 300 の内容は実質的に変更されず、そのまま暗号化制御情報部 100 となる。

【0043】(2) 暗号する箇所を 1 つのみ指定可能な実施例

図 12 (a) は業務プログラム 3-1 ~ 3-m から部分的暗号化装置 5 に入力される情報フレームのフォーマット例を示す図である。この例の情報フレームは、暗号化制御情報部 500 と、複数のユーザデータから構成されるデータ部 600 とから構成されている。暗号化制御情報部 500 は、データ部 600 に格納された一連のユーザデータのうち暗号化対象となるデータの開始位置 501 及びそのバイト数 502 を指定した 1 つの暗号化箇所指定情報 503 から構成される。開始位置 501、バイト数 502 のサイズは固定長である。図 12 (b) に、開始位置 501 及びバイト数 502 とユーザデータとの関連を示す。開始位置 501 としては、例えば情報フレームの先頭の 1 バイト（つまり開始位置 501 の先頭バイト）目を 0 バイト目とした場合の、当該ユーザデータまでのバイト数で表現される。なお、本実施例では、部分的復号化装置 6 から業務プログラム 3-1 ~ 3-m に入力される情報フレームも図 12 (a) の形式としている。

【0044】他方、図 12 (c) は部分的暗号化装置 5 からデータ送受信装置 4 に入力される情報フレームのフォーマット例を示す図である。この例の情報フレームは、復号化制御情報部 700 と、複数のユーザデータから構成されるデータ部 800 とから構成されている。復号化制御情報部 700 は、データ部 800 に格納された一連のユーザデータのうち復号化対象となるデータの開始位置 701 及びそのバイト数 702 を指定した 1 つの復号化箇所指定情報 703 から構成される。開始位置 701、バイト数 702 のサイズは固定長である。開始位置 701 としては、例えば情報フレームの先頭の 1 バイト（つまり開始位置 701 の先頭バイト）目を 0 バイト目とした場合の、当該ユーザデータまでのバイト数で表現される。なお、本実施例では、データ送受信装置 4 から部分的復号化装置 6 に入力される情報フレームも図 12 (c) の形式としている。

【0045】(A) 暗号化によりデータサイズが拡大する場合

【0046】(ア) 暗号化

この場合の部分的暗号化装置 5 の処理の一例を図 13 のフローチャートに示す。何れかの業務プログラム 3-1 ~ 3-m から図 12 (a) に示したような形式の情報フレームが送られると、入力手段 51 がそれを入力し（ステップ S41）、暗号化制御手段 52 に伝達する。暗号化制御手段 52 は、情報フレームの暗号化制御情報部 500 を解析し（ステップ S42）、解析結果を制御テーブルに設定する（ステップ S43）。

【0047】例えば、図 14 (a) に示すように、各々 32 バイト、32 バイト、16 バイト、16 バイト、16 バイトである 5 つのユーザデータ U1、U2、U3、

11

U4、U5を含むデータ部600と、ユーザデータU3を暗号化対象として指定した暗号化制御情報部500とから構成される情報フレームの場合、個数、開始位置のサイズを例えば1バイト固定とすると、情報フレームの先頭から66～82バイト目のユーザデータU3が暗号化対象データであり、ユーザデータU3の前後のデータ（ユーザデータU1、U2、U4、U5）は暗号化対象データでないで、例えば図15に示すような3つのエントリE1、E2、E3を持つ制御テーブル902を生成し、開始位置、バイト数、暗号化の有無の欄にそれぞれ図示する値を設定する。なお、この時点では、暗号化後のバイト数の欄はNULLである。

【0048】次に暗号化制御手段52は、制御テーブル902の暗号化の有無の欄が「有」になっているエントリE2について、該当する箇所のデータをデータ部600から取り出し、暗号手段53に与えることにより暗号化する（ステップS44）。

【0049】次に暗号化制御手段52は、暗号化後のデータサイズを図15に示すように、エントリE2の暗号化後のバイト数の欄に設定する（ステップS45）。

【0050】次に暗号化制御手段52は、図15の制御テーブル902の暗号化の有無の欄が「有」になっているエントリE2の開始位置「66」と暗号化後のバイト数「24」との組を復号化箇所指定情報703とした復号化制御情報部700を生成する（ステップS46）。これにより、図14（b）に示す復号化制御情報部700が生成される。

【0051】次に暗号化制御手段52は、図15の制御テーブル902のエントリE1から順にエントリE3まで、そのエントリの暗号化の有無の欄が「有」であれば暗号化後のデータを、「無」であれば、制御テーブル902の開始位置の欄とバイト数の欄とで特定される入力情報フレーム上の元のデータを、データ部の先頭から順に詰め込んで、データ部800を生成する（ステップS47）。これにより、図14（b）に示すデータ部800が生成される。

【0052】以上のようにして復号化制御情報部700とデータ部800とから構成される情報フレームが生成されると、出力手段54が、送り先および送り元の情報と共に情報フレームをデータ送受信装置4に送る（ステップS48）。

【0053】（イ）復号化

この場合の部分的復号化装置6の処理の一例を図16のフローチャートに示す。データ送受信装置4から図12（c）に示したような形式の情報フレームが送られると、入力手段61がそれを入力し（ステップS51）、復号化制御手段62に伝達する。復号化制御手段62は、情報フレームの復号化制御情報部700を解析し（ステップS52）、解析結果を制御テーブルに設定する（ステップS53）。

12

【0054】例えば、入力された情報フレームが図14（b）に示した情報フレームであった場合、情報フレームの先頭から66～90バイト目のユーザデータU3'が復号化対象データであり、ユーザデータU3'の前後のデータ（ユーザデータU1、U2、U4、U5）は復号化対象データでないで、例えば図17に示すような3つのエントリE1、E2、E3を持つ制御テーブル903を生成し、開始位置、バイト数、復号化の有無の欄にそれぞれ図示する値を設定する。なお、この時点では、復号化後のバイト数の欄はNULLである。

【0055】次に復号化制御手段62は、制御テーブル903の復号化の有無の欄が「有」になっているエントリE2について、該当する箇所のデータをデータ部800から取り出し、復号手段63に与えることにより復号化する（ステップS54）。

【0056】次に復号化制御手段62は、復号化後のデータサイズを図15に示すように、エントリE2の復号化後のバイト数の欄に設定する（ステップS55）。

【0057】次に復号化制御手段62は、図17の制御テーブル903の復号化の有無の欄が「有」になっているエントリE2の開始位置「66」と復号化後のバイト数「16」との組を暗号化箇所指定情報503とした暗号化制御情報部500を生成する（ステップS56）。これにより、図14（a）に示す暗号化制御情報部500が生成される。

【0058】次に復号化制御手段62は、図17の制御テーブル903のエントリE1から順にエントリE3まで、そのエントリの復号化の有無の欄が「有」であれば復号化後のデータを、「無」であれば、制御テーブル903の開始位置の欄とバイト数の欄とで特定される入力情報フレーム上の元のデータを、データ部の先頭から順に詰め込んで、データ部600を生成する（ステップS57）。これにより、図14（a）に示すデータ部600が生成される。

【0059】以上のようにして暗号化制御情報部500とデータ部600とから構成される情報フレームが生成されると、出力手段64が、送り元の情報と共に送り先の業務プログラムに送る（ステップS58）。

【0060】（B）暗号化によりデータサイズが拡大しない場合

【0061】（ア）暗号化

この場合の部分的暗号化装置5の処理の一例を図18のフローチャートに示す。何れかの業務プログラム3-1～3-mから図14（a）に示したような形式の情報フレームが送られると、入力手段51がそれを入力し（ステップS61）、暗号化制御手段52に伝達する。暗号化制御手段52は、情報フレームの暗号化制御情報部500を解析し、その開始位置501とバイト数502とで特定される箇所のデータを、データ部600から取り出し（ステップS62）、暗号手段53に与えることに

より暗号化する（ステップS 6 3）。次に、生成された暗号データで、データ部6 0 0の元の箇所を上書きする（ステップS 6 4）。そして、データ部6 0 0が上書きされた情報フレームを、出力手段5 4により、送り先および送り元の情報と共にデータ送受信装置4に送出する（S 6 5）。

【0 0 6 2】このように暗号化によってデータサイズが拡大せず同一サイズとなる場合、入力された情報フレームの暗号化制御情報部5 0 0の内容は実質的に変更されず、そのまま復号化制御情報部7 0 0となる。

【0 0 6 3】（イ）復号化

この場合の部分的復号化装置6の処理の一例を図1 9のフローチャートに示す。データ送受信装置4から図1 2（c）に示したような形式の情報フレームが送られると、入力手段6 1がそれを入力し（ステップS 7 1）、復号化制御手段6 2に伝達する。復号化制御手段6 2は、情報フレームの復号化制御情報部7 0 0を解析し、その開始位置7 0 1及びバイト数7 0 2で特定される箇所のデータを、データ部8 0 0から取り出し（ステップS 7 2）、復号手段6 3に与えることにより復号化する（ステップS 7 3）。次に、生成された復号データで、データ部8 0 0の元の箇所を上書きする（ステップS 7 4）。そして、データ部8 0 0が上書きされた情報フレームを、出力手段6 4により、送り元の情報と共に送り先の業務プログラムに送出する（S 7 5）。

【0 0 6 4】このように復号化によってデータサイズが拡大せず同一サイズとなる場合、入力された情報フレームの復号化制御情報部7 0 0の内容は実質的に変更されず、そのまま暗号化制御情報部5 0 0となる。

【0 0 6 5】以上の実施の形態は、情報処理装置間で送受信されるデータに対する暗号化、復号化に本発明を適用したが、情報処理装置上の業務プログラムがデータを暗号化してローカルな記憶装置に記録する場合の記録データの暗号化、記録されたデータの復号化にも本発明は適用可能である。

【0 0 6 6】

【発明の効果】以上説明したように本発明によれば以下のような効果が得られる。

【0 0 6 7】一連のデータ中の暗号化したい箇所をよりきめ細かく指定することができる。その理由は、一連のデータのうち暗号化したいデータの開始位置だけでなく、その長さも指定することができるからであり、また、開始位置と長さを複数組指定することができるからである。

【0 0 6 8】このように暗号化したい箇所をきめ細かく指定できるため、必要最小限の暗号化が可能となり、暗号化処理時間の大幅な短縮が可能となる。

【図面の簡単な説明】

【図1】本発明を適用した情報処理装置の一例を示すブロック図である。

【図2】部分的暗号化装置の構成例を示すブロック図である。

【図3】部分的復号化装置の構成例を示すブロック図である。

【図4】情報フレームのフォーマットの一例を示す図である。

【図5】部分的暗号化装置の処理例を示すフローチャートである。

【図6】情報フレームの具体例を示す図である。

10 【図7】部分的暗号化装置が使用する制御テーブルの例を示す図である。

【図8】部分的復号化装置の処理例を示すフローチャートである。

【図9】部分的復号化装置が使用する制御テーブルの例を示す図である。

【図1 0】部分的暗号化装置の処理例を示すフローチャートである。

【図1 1】部分的復号化装置の処理例を示すフローチャートである。

20 【図1 2】情報フレームのフォーマット例を示す図である。

【図1 3】部分的暗号化装置の処理例を示すフローチャートである。

【図1 4】情報フレームの具体例を示す図である。

【図1 5】部分的暗号化装置が使用する制御テーブルの例を示す図である。

【図1 6】部分的復号化装置の処理例を示すフローチャートである。

30 【図1 7】部分的復号化装置が使用する制御テーブルの例を示す図である。

【図1 8】部分的暗号化装置の処理例を示すフローチャートである。

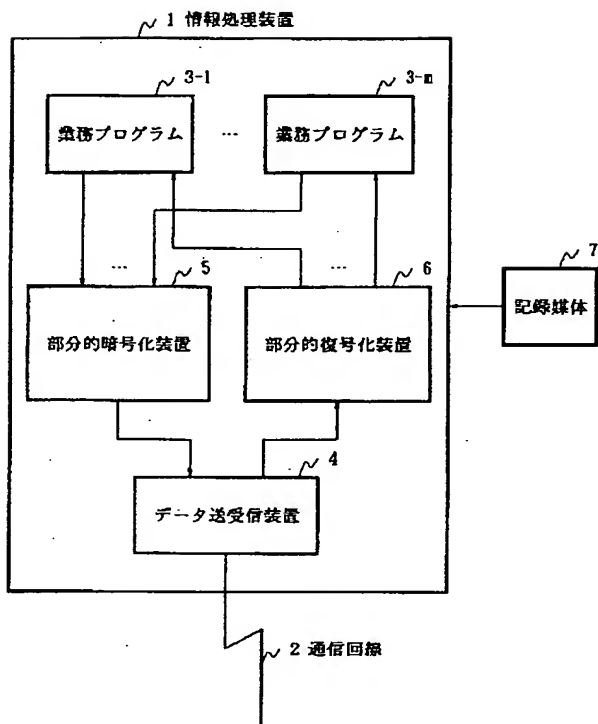
【図1 9】部分的復号化装置の処理例を示すフローチャートである。

【図2 0】従来の問題点の説明図である。

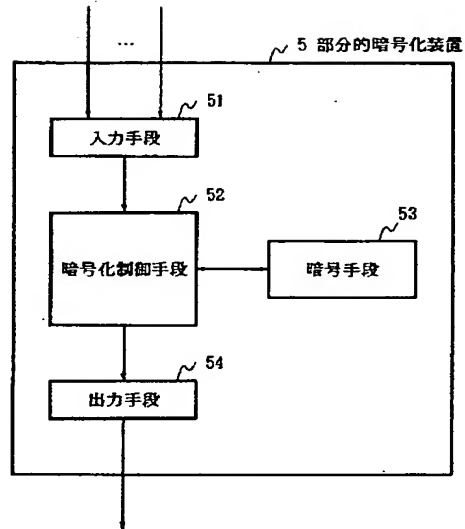
【符号の説明】

- 1…情報処理装置
- 2…通信回線
- 3-1～3-m…業務プログラム
- 40 4…データ送受信装置
- 5…部分的暗号化装置
- 6…部分的復号化装置
- 7…記録媒体
- 5 1, 6 1…入力手段
- 5 2…暗号化制御手段
- 5 3…暗号手段
- 5 4, 6 4…出力手段
- 6 2…復号化制御手段
- 6 3…復号手段

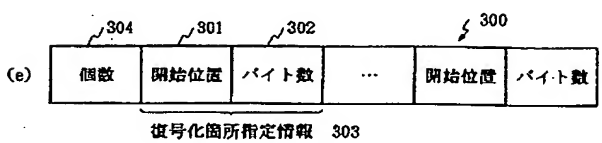
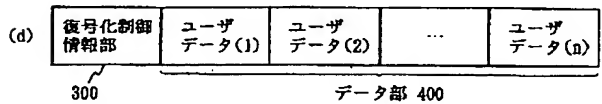
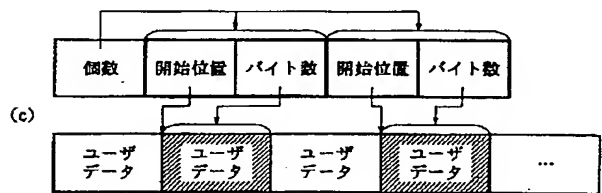
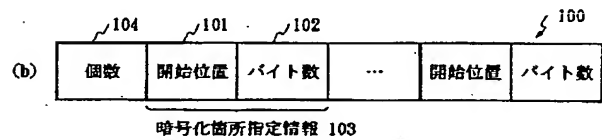
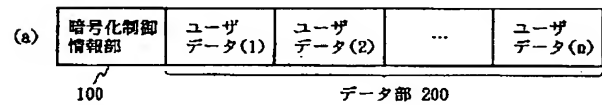
【図 1】



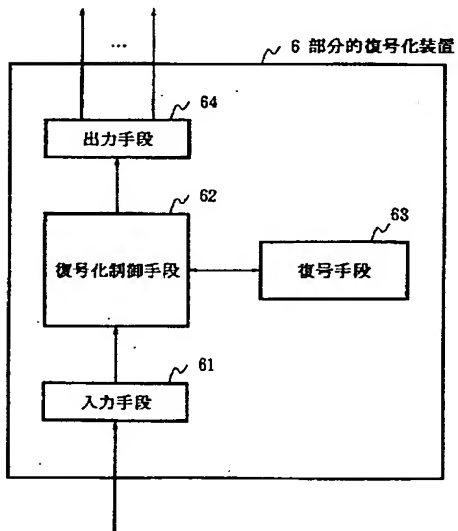
【図 2】



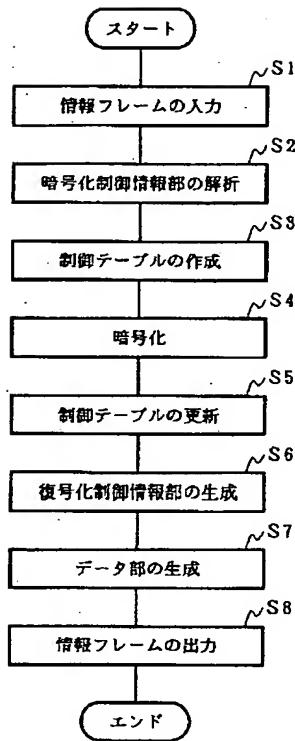
【図 4】



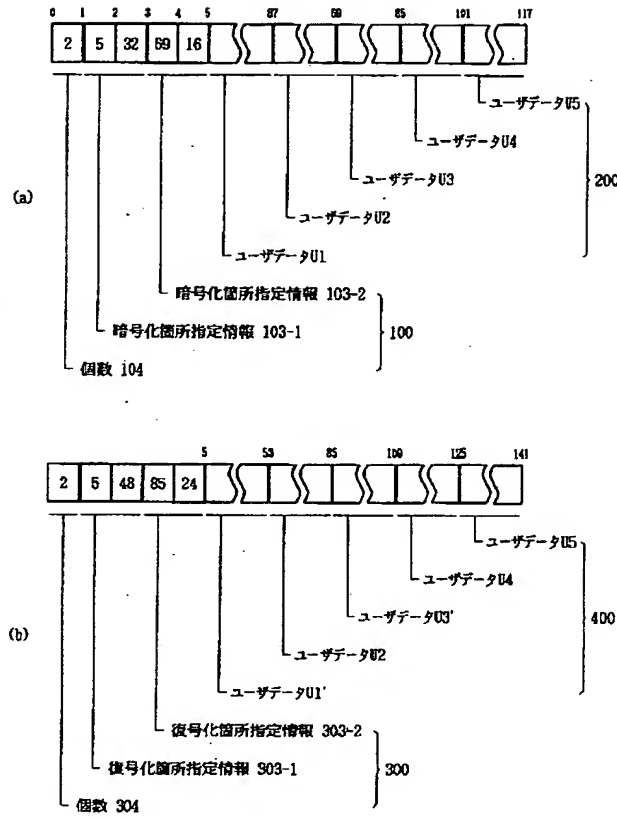
【図 3】



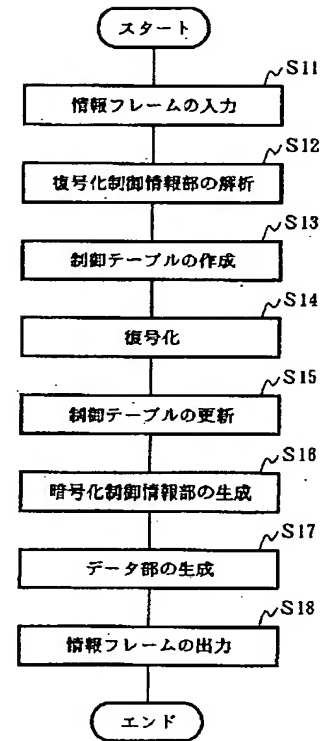
【図 5】



【図 6】



【図 8】



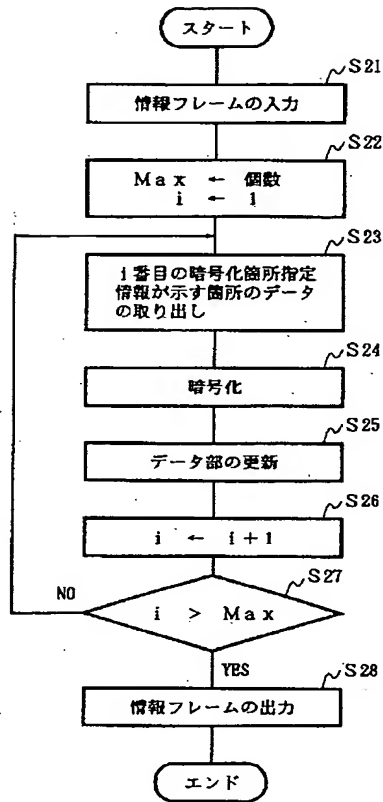
【図 7】

開始位置	バイト数	暗号化の有無	暗号化後の開始位置	暗号化後のバイト数
5	32	有	5	48
37	32	無	53	—
69	16	有	85	24
85	32	無	109	—

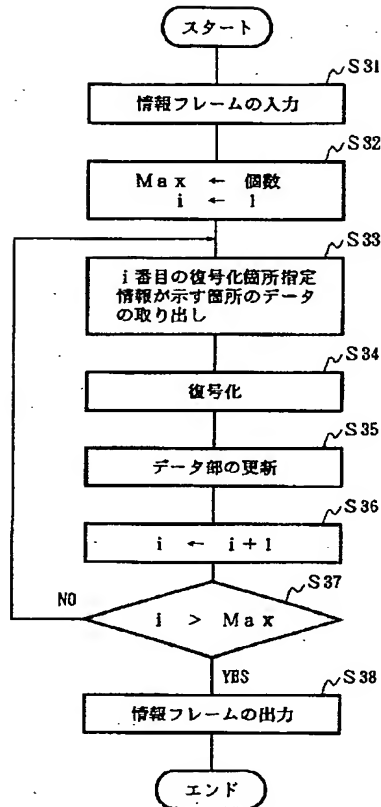
【図 9】

開始位置	バイト数	復号化の有無	復号化後の開始位置	復号化後のバイト数
5	48	有	5	32
53	32	無	37	—
85	24	有	69	16
109	32	無	85	—

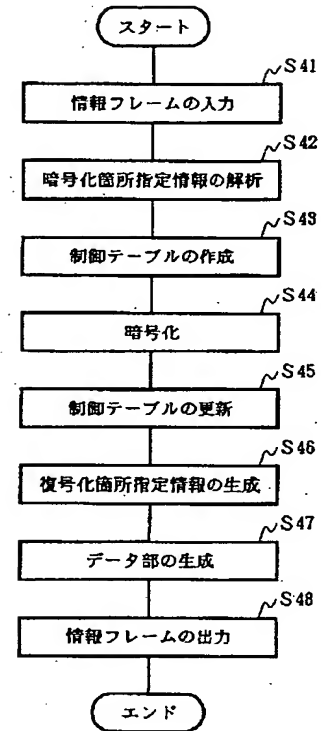
【図 10】



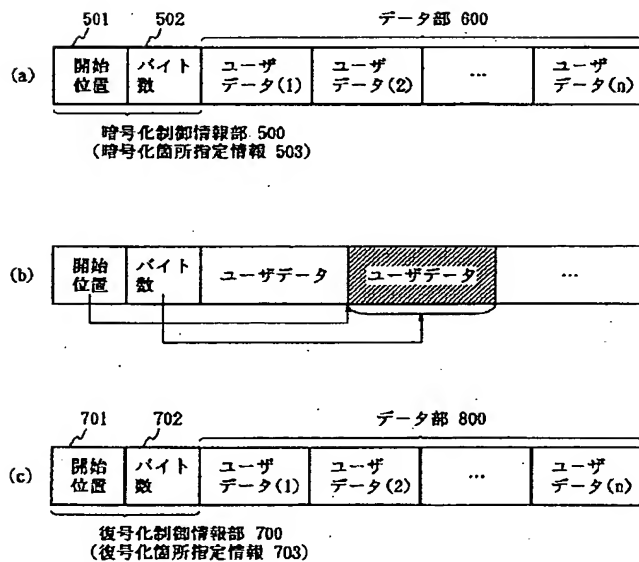
【図 11】



【図 13】



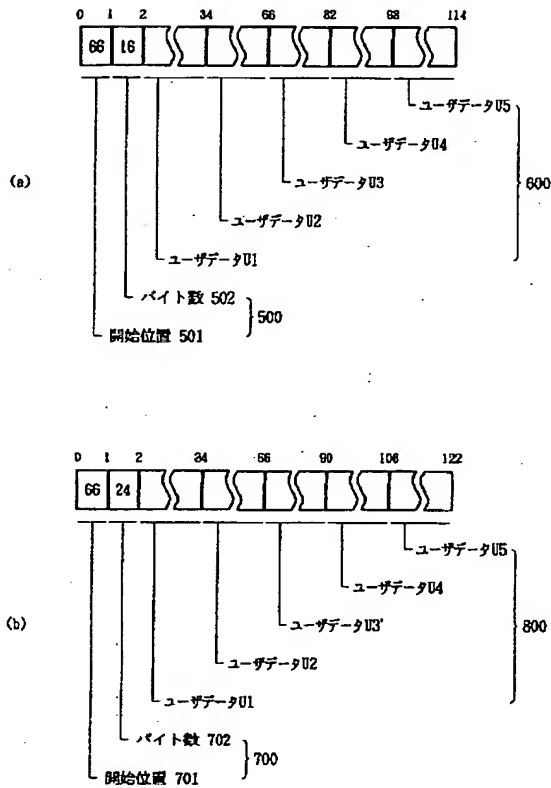
【図 12】



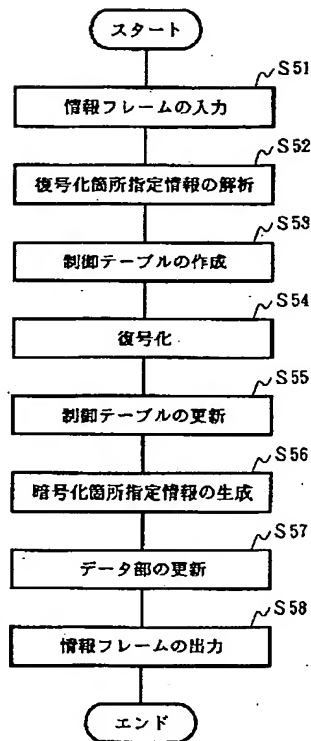
【図 15】

開始位置	バイト数	暗号化の有無	暗号化後のバイト数
2	64	無	—
66	16	有	24
82	32	無	—

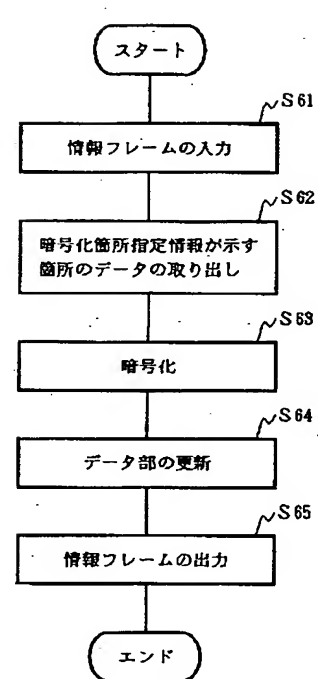
【図 14】



【図 16】



【図 18】



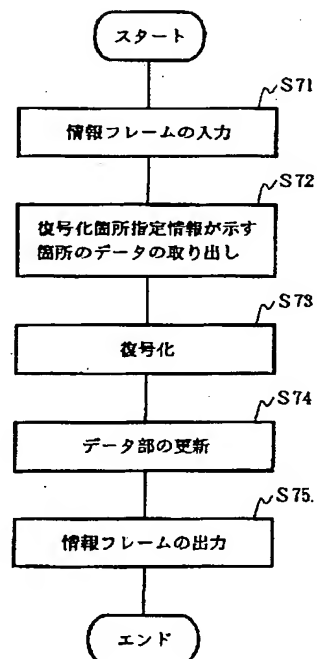
【図 17】

903

開始位置	バイト数	復号化の有無	復号化後のバイト数
2	64	無	-
66	24	有	16
90	32	無	-

E1
E2
E3

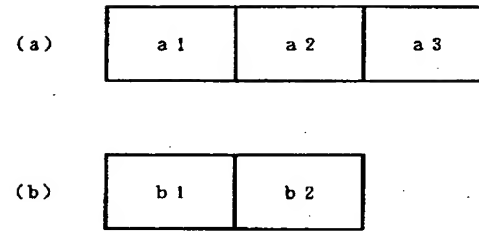
【図 19】



(13)

特開平 1 1 - 3 4 4 9 2 5

【図 2 0】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.